A publication of the DCIS Northeast Field Office

TECHNOBABBLE

The DCIS Cyber Crime Newsletter

TECHNOBABBLE
Volume 2, Issue 5

September, 2001

This issues suggested computer crime bookmarks:

Anti-Child Pornography.org
http://www.antichildporn.org

Computer Crime Research Resources:
http://mailer.fsu.edu/~btf1553/ccrr/welcome.htm

Computer Crime and Legal Resource Directory:
http://www.cpsr.org/cpsr/privacy/crime/crime.html

Inside this issue:

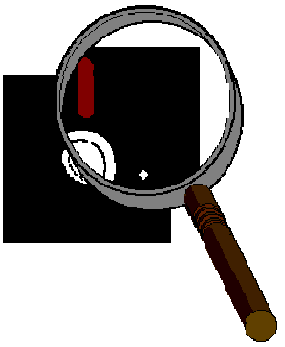
Army Employee Pleas to Child Porn Violations

On August 7, 2001, Louis O. Lee pled guilty in U.S. District Court, Baltimore, MD, to a single count of transportation and shipment of child pornography interstate by means of computer.

Lee was indicted by a Federal grand jury on April 30, 2001. The indictment charged Lee, a program analyst with the Department of Army, Army Research Laboratory (ARL), Adelphi, MD, with downloading images of child pornography that traveled in interstate commerce to his computer at the ARL. The investigation revealed Lee saved graphic images to 15 subdirectories in his computer and that almost all of those folders had their file extensions renamed to appear as spreadsheets or other data files in an attempt to prevent the possibility of discovery.

Lee faces a maximum sentence of 5 years in prison and a fine of not more than $250,000,or both. A sentencing date has not yet been set.

The investigation was conducted jointly by the Defense Criminal Investigative Service's Mid-Atlantic Field Office and the Federal Bureau of Investigation. The United States Attorney Office, District of Maryland, Greenbelt, MD, is handling prosecution of this matter.



Administrators Urged to Upgrade SendMail

Linux and Unix system administrators are being urged to upgrade some versions of the popular Sendmail e-mail server software utilized worldwide due to the identification of potential security issues which can provide a doorway for hackers.

Institutions which regularly provide individuals with shell accounts are most susceptible to the problem, since an attacker would need to gain command-line access to a server in order to exploit the vulnerability.

A recent report from Cade Cairns, Security Focus Threat Analysis Team, indicates that that intruders who gain access to Sendmail from the command line of vulnerable systems could gain root privileges on a system by supplying a series of instructions at the command prompt..

Cairns reported that the vulnerability was present in releases of the consortium's Sendmail versions above 8.10.0 and through 8.11.5 and in all beta versions of 11.12.0.

The problem is compounded by the fact that Sendmail is so widely utilized throughout the Internet community. Unix administrators have been utilizing the utility since the 1980s, and the open-source version of the software is included with a wide variety of Unix and Linux distributions.

For more information relative to referenced Sendmail security concerns, check out:

http://www.sendmail.org

SENDMAIL

Open Source Napster Clones

The Gnutella Network and Potential Copyright Infringement Implications

By Special Agent Jim Ives, DCIS Boston Resident Agency

Most individuals with an interest in computer crime are well aware of on-going battles between the recording industry and the peer to peer audio file sharing service known as Napster. At present time, the future of Napster's existence (at least in its previous form) is questionable due to recording industry lawsuits alleging that the service has violated various copyright regulations by making high quality audio tracks saved in a compressed format known as MPEG3 (or MP3 for short) freely available to the public.

In response to the recording industry's allegations, many individuals argued that shutting down Napster would simply result in the organization being replaced by clones offering "Napster-like" services. In fact, the code required to develop Napster replacements was already readily available and in use prior to legal actions which resulted in suspension of Napster's services.

The Birth of Gnutella

On March 14, 2000, at 11:31 AM EST, a message posted to an underground hacker website claimed that America Online's Nullsoft division had released an "open-source Napster clone" named Gnutella, capable of searching for and downloading not only MP3 audio tracks, but any kind of computer file. Subsequent reports indicated that Nullsoft's distribution of the Gnutella utility had ceased, suggesting that the reason for this was the potential threat that Gnutella posed to record labels which were discussing potential mergers with AOL. However, in the time that the software was available from the Nullsoft site, several thousand downloads took place, and various third parties soon set to work cloning the Nullsoft version of the Gnutella program. These clones were all written to be compatible with the Gnutella protocol established by the Nullsoft program, and could therefore communicate with each other and with the original Nullsoft client. As people began to run these clones as well as unauthorized copies of the original client, a network of Gnutella-compatible applications grew and began to communicate in the decentralized manner that the Gnutella protocol specified. This network, which has grown significantly over the past year, has come to be known as the Gnutella Network.

All computers running a program utilizing the Gnutella protocol are said to be on the Gnutella Network (or "gNet"). On the World Wide Web, each computer is connected to only one other computer at a time. On the Gnutella Network, a user is connected to several other computers at once. Information can be received from many sources simultaneously. Each computer on the Gnutella Network is connected to a number of other computers (peers). Each of these peers is connected to several other computers. This process continues indefinitely. If a user is connected to 4 computers, each of which are connected to 4 other computers, the total number of computers with which the user is able to communicate with is 4 + 4*4=20. In this case, the messages only travel 2 "hops" along the network.The number of "hops" in a search request is also known as its "time to live" or TTL. In this case, the user's TTL is 2. If we expand the above example to set our hypothetical user's TTL to 3, and each computer in the network is connected to 4 new computers, the total number of computers with which she can communicate with is 4 + 4*4 + 4*4*4 = 84. Therefore, the number of computers with which the user can communicate grows exponentially in relation to the increase in TTL of her search requests. The Gnutella Network, in theory at least, would be able to reach every computer on the Internet through this system of connections.

"The Gnutella Network, in theory at least, would be able to reach every computer on the Internet through this system of connections."

Potential for Abuse

So what elements of the Gnutella network make the protocol a more serious threat than Napster to those industries concerned with copyright violations?

1) First and foremost, we must reiterate the fact that **no single individual or organization**

Open Source Napster Clones (continued)

"At any given moment, Gnutella users are 'sharing' copyrighted electronic books (E-books), audio books, proprietary software, decoded DVD videos, credit card numbers, and counterfeit 'key codes' utilized to register software manufactured by companies such as Microsoft."

maintains the Gnutella network. Gnutella simply functions as a protocol which can be utilized on individual computer systems ranging from PC's connected to the Internet via 56k modems, to more powerful servers utilized by places of business, government institutions, and universities. Since no single entity controls Gnutella, it is next to impossible to shut the service down. In the case of Napster, a court order targeting the administrators of the service could be issued to force the entity to cease operations. In the case of Gnutella, the court order would have to be issued to each and every individual who chooses to utilize the protocol on their computer system!

2) Gnutella's file distribution functionality is not limited to audio files. The protocol can be utilized to share any type of file available. A brief glimpse of file exchange traffic between Gnutella users reveals that the recording industry is not the only group which needs to be concerned with distribution of copyrighted material via the net. At any given moment, Gnutella users are "sharing" copyrighted electronic books (E-books), audio books, proprietary software, decoded DVD videos, credit card numbers, and counterfeit "key codes" utilized to register software manufactured by companies such as Microsoft. As more and more users graduate to high bandwith connections, and the prevalence of net based video increases, it is only a matter of time before the motion picture industry begins to feel the same threat previously reserved for the recording industry.

3) Unlike Napster, the Gnutella protocol is also frequently utilized as a method of distributing massive amounts of pornography, to include child porn.

4) Investigators will find that tracking Gnutella users will be incredibly difficult. By way of example, assume two users utilizing the Gnutella protocol on their personal computers decide to exchange classified documents, or documents containing protected intellectual property. The users could simply connect to the Internet, activate the protocol, and exchange the files. Since no entity controls the service, law enforcement would have no single source to approach in order to obtain connection logs showing the file transfers. Officials would have to rely upon logs maintained by individual Internet Service Providers which the users utilized. As we know, many ISP's only maintain such logs for days or hours, if they maintain logs at all.

5) New front ends are now available which make utilizing Gnutella exceedingly simple. One of the strengths of Napster was its simple to use interface. Users with little (if any) computer experience could download software, install it on their computer, and begin trading MP3's with individuals throughout the world. Gnutella users are now offered the same level of simplicity. One such front end, known as Lime Wire, could at first glance be mistaken for Napster's previous interface. There is, however, one key distinction: at the user's discretion, Lime Wire's search engine will not only scour the Gnutella network for MP3's, but will do the same for other popular file formats, to include documents, programs, images, and video.

6) If history dictates, the open source nature of Gnutella will ensure its survival for quite some time. Since source code for the protocol is readily available, it will undoubtely exist for years to come, and mutate into various incarnations.

Conclusions

The evolution of Gnutella mimics a trend which has become all too common in the on-line world. The protocol provides a useful tool in providing remote users with the ability to simplify file transfer via peer to peer networking, a function which could potentially benefit both individual Internet users and the business community alike. However, a certain number of users seem insistent upon converting potentially beneficial applications into tools for committing crimes. This fact, combined with Gnutella's unique capability to connect remote computers without the use of a central server, is sure to provide law enforcement officials with an especially challenging hurdle for years to come.

For more information relative to Gnutella, Limewire, and open source peer to peer networking, check out the following links:

http://www.gnutella.co.uk

http://www.gnutella.wego.com

http://www.zeropaid.com

http://dss.clip2.com

http://www.gnutellanews.com

http://www.gnutelliums.com

http://www.limewire.com

This Issues Suggested Reading

Incident Response: Investigating Computer Crime

Looking for a book that covers it all—everything from responding to computer intrusions to evidence handling and forensic analysis? *Incident Response: Investigating Computer Crime* may be the book for you!

According to Amazon.com's editorial review of the text, "Anti-attack procedures are presented with the goal of identifying, apprehending, and successfully prosecuting attackers. The advice on carefully preserving volatile information, such as the list of processes active at the time of an attack, is easy to follow. The book is quick to endorse tools, the functionalities of which are described so as to inspire creative applications.

Information on bad-guy behavior is top quality as well, giving readers knowledge of how to interpret logs and other observed phenomena. Mandia and Prosise don't--and can't--offer a foolproof guide to catching crackers in the act, but they do offer a great 'best practices' guide to active surveillance."

Mark J. Zwillinger, former trial attorney with the U.S. Department of Justice Computer Crime and Intellectual Property Section concurs with Amazon.com's view relative to the usefulness of the book. According to Zwillinger, *Incident Response* is "the most comprehensive guide to incident response ever published."

Title:

Incident Response: Investigating Computer Crime

Authors:

Kevin Mandia & Chris Prosise

Cost:

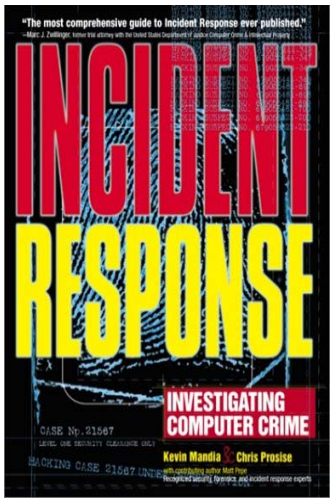
$39.99

ISBN:

0-07-213182-9

Publisher:

Osborne



Know the Code!

Common Federal Statutes Utilized in Prosecuting Computer Crime
By Special Agent Jim Ives, DCIS Boston Resident Agency

18 USC 1029–Fraud and Related Activity in Connection with Access Devices

This issues 'commonly utilized statute' is 18 USC 1029, which addresses fraud involving access devices.

The following language defines offenses covered by the statute:

(a) Whoever -

(1) knowingly and with intent to defraud produces, uses, or traffics in one or more counterfeit access devices;
(2) knowingly and with intent to defraud traffics in or uses one or more unauthorized access devices during any one-year period, and by such conduct obtains anything of value aggregating $1,000 or more during that period;
(3) knowingly and with intent to defraud possesses fifteen or more devices which are counterfeit or unauthorized access devices;
(4) knowingly, and with intent to defraud, produces, traffics in, has control or custody of, or possesses device-making equipment;
(5) knowingly and with intent to defraud effects transactions, with 1 or more access devices issued to another person or persons, to receive payment or any other thing of value during any 1-year period the aggregate value of which is equal to or greater than $1,000;
(6) without the authorization of the issuer of the access device, knowingly and with intent to defraud solicits a person for the purpose of - (A) offering an access device; or (B) selling information regarding or an application to obtain an access device;
(7) knowingly and with intent to defraud uses, produces, traffics in, has control or custody of, or possesses a telecommunications instrument that has been modified or altered to obtain unauthorized use of telecommunications services;
(8) knowingly and with intent to defraud uses, produces, traffics in, has control or custody of, or possesses a scanning receiver;
(9) knowingly uses, produces, traffics in, has control or

Know the Code! (continued)

custody of, or possesses hardware or software, knowing it has been configured to insert or modify telecommunication identifying information associated with or contained in a telecommunications instrument so that such instrument may be used to obtain telecommunications service without authorization; or

(10) without the authorization of the credit card system member or its agent, knowingly and with intent to defraud causes or arranges for another person to present to the member or its agent, for payment, 1 or more evidences or records of transactions made by an access device; shall, if the offense affects interstate or foreign commerce, be punished as provided in subsection (c) of this section.

Penalties for violations of the statute range from fines to 20 years imprisonment.

At first glance, one may question why a statute which was obviously designed to battle credit card fraud can be effectively utilized to combat computer related crime. The answer lies in the open ended terms used throughout the statute. For example, the Department of Justice defines "access devices" as "any card, plate, code, account number, electronic serial number, mobile identification number, personal identification number, or other telecommunications service, equipment, or instrument identifier, or other means of account access that can be used, alone or in conjunction with another access device, to obtain money, goods, services, or any other thing of value, or that can be used to initiate a transfer of funds (other than a transfer originated solely by paper instrument)." This definition has been interpreted to include passwords which can be utilized to illegally access computer networks. Since the statute provides sanctions for possession and trafficking of "unauthorized" access devices, a hacker who has collected a number of user id / password combinations through illegally accessing computer networks subjects himself not only to potential prosecution under 18 USC 1030, Fraud and Related Activity in Connection with Computers (see Technobabble Volume 2, Issue 4 for details), but could also be charged for violations of 18 USC 1029. In fact, many prosecutors opt to charge hackers with violations of both statutes, which can potentially result in significant penalties. If the hacker were to utilize the password to illegally access a computer network, and subsequently caused significant financial damages as a result of the incident (i.e.costs related to rebuilding the compromised system), penalties can increase substantially.

Another example of potential use in prosecuting computer crime lies in the interpretation of the term "scanning receiver." According to DoJ, a scanning receiver is defined as a "device or apparatus that can be used to intercept a wire or electronic communication in violation of chapter 119 or to intercept an electronic serial number, mobile identification number, or other identifier of any telecommunications service, equipment, or instrument." One could argue that sniffers, commonly utilized by hackers to illegally intercept network communications (such as passwords), could qualify as a "scanning receiver" for purposes of prosecution via 18 USC 1029.

"This definition has been interpreted to include passwords which can be utilized to illegally access computer networks."

DoD Temporarily Pulls Plug in Response to Code Red

Although the threat posed by the so-called 'Code Red' virus seems to have lessened, Department of Defense (DoD) components are still actively monitoring potential impacts upon the department's massive computer networks.

Initial defensive efforts, coordinated by the U.S. Space Command in Colorado Springs, CO, involved instructing DoD components to disconnect many publicly accessible military and civilian DoD web servers. DoD system administrators were also instructed to apply patches to their servers so as to avoid potential infestation.

The first sign of attack was identified on July 19th. DoD officials took immediate action in addressing the issue in order to mitigate the potential results should the virus successfully penetrate thousands of its' servers located throughout the world. Normal network operations were re-established on July 24th.

Air Force Gen. Ralph E. Eberhart, head of Space Command, commented that, "the comparison with how the Pentagon deals with that kind of problem today compared with three or four years ago is enormously more positive. That is a good thing, because it is enormously more dangerous these days."

A publication of the DCIS Northeast Field Office

Defense Criminal Investigative Service
Northeast Field Office
10 Industrial Highway, Bldg. G, Mail Stop 75
Lester, PA 19113

Phone: (610) 595-1900
Fax: (610) 595-1934

Send comments to: Jives@dodig.osd.mil

We're on the Web!
www.dodig.osd.mil/dcis/dcismain.html

The Defense Criminal Investigative Service

"Protecting America's Warfighters"

The Defense Criminal Investigative Service is the investigative arm of the U.S. Department of Defense, Office of the Inspector General. As such, DCIS investigates criminal, civil, and administrative violations impacting the Defense Department. Typically, DCIS investigations focus upon computer crime involving U.S. military and civilian DoD systems, contract procurement fraud, bribery and corruption, health care fraud, anti-trust investigations, significant thefts of government property, export enforcement violations, environmental violations, and other issues that impact the integrity and effectiveness of the U.S. Department of Defense.

If you encounter issues that impact the U.S. Department of Defense, please call the DCIS office within your region.

DCIS Northeast Field Office.
10 Industrial Hwy., Bldg. G
Lester, PA 19113
Phone: (610) 595-1900
Fax: (610) 595-1934

DCIS Boston Resident Agency
Rm. 327, 495 Summer Street
Boston, MA 02210
Phone: (617) 753-3044
Fax: (617) 753-4284

DCIS Hartford Resident Agency
525 Brook Street, Suite 205
Rocky Hill, CT 06067
Phone: (860) 721-7751
Fax: (860) 721-6327

DCIS New Jersey Resident Agency
Wick Plaza 1, 100 Dey Pl., Ste. 102
Edison, NJ 08817
Phone: (732) 819-8455
Fax: (732) 819-9430

DCIS New York Resident Agency
One Huntington Quad, Suite 2C01
Melville, NY 11747
Phone: (516) 420-4302
Fax: (516) 420-4316

DCIS Pittsburgh Post of Duty
1000 Liberty Ave., Ste. 1310
Pittsburgh, PA 15222
Phone: (412) 395-6931
Fax: (412) 395-4557

DCIS Syracuse Resident Agency
441 S. Selina St., Ste. 304
Syracuse, NY 13202
Phone: (315) 423-5019
Fax: (315) 423-5099